Certificate of Mailing/Facsimile 37 CFR 1.8(a)

I hereby certify that this correspondence is being:

_____ deposited with the United States Postal Service as first class mail in an envelope with sufficient postage addressed to:

COMMISSIONER OF PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

__X__ transmitted by facsimile to 571 273 8300

on March 2 2006

By David E. McConnell

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	Date: March 2, 2006
D.C. Challener et al	:	Group Art Unit: 2137
Serial Number: 10/063,988	:	Examiner: A.S. Abyaneh
Filed: 31 May 2002	:	INTERNATIONAL BUSINESS MACHINES CORPORATION
Title: Assurance of Authentication in a Computer System Apparatus and Method	:	Intellectual Property Law Dept. D-YXSA B-002/2 P.O. Box 12195
	:	Research Triangle Park, NC 27709

Declaration of prior invention to overcome cited patent (37 C.F.R. 1.131)

The Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This declaration is to establish completion of the invention in this application in the United States, at a date prior to September 4, 2001, the effective date of the Chen et al U.S. Published Patent application 2003/0046542 cited by the Examiner. This declaration is presented in response to the first Official Action in which the Chen et al application has been cited, mailed December 12, 2005.

The persons making this declaration are the inventors.

The attached Invention Disclosure document is submitted as evidence to establish the date of completion of the invention of this application. The dates appearing on the original document have been redacted. However, the declarants state that the redacted dates are well prior to September 4, 2001.

The declarants further state that conception of the invention was followed by due diligence from the time of conception to a time just prior to the effective date of the reference, up to the actual reduction to practice of the invention and the filing of this application.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false

statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: David Carroll Challener

Signature:

Date: 3/1/06

Inventor: James Hoff

Signature:

Date: 3/1/2006

Inventor: Howard J. Locker

Signature:

Date 3/1/2006

Inventor: James P. Ward

Signature:

Date:

Disclosure RPS8-2001-0130

Prepared for and/or by an IBM Attorney - IBM Confidential

Created By James Hoff On 01:05:32 PM EDT
Last Modified By Maura R Roberts On 10:52:48 PM EDT
Archived on 05/17/2003

Required fields are marked with the asterisk (*) and must be filled in to complete the form .

***Title of disclosure (In English)**
Secure Pin entry for TCPA

Summary

Status	Final Decision (File)
Final deadline	
Final deadline reason	
Docket family	RPS9-2002-0047
* Processing location	Raleigh - RPS
* Functional area	(DESKTOP SYSTEMS) DESKTOP SYSTEMS
Attorney/Patent professional	George Grosser/Raleigh/IBM
Invention development team (IDT)	Chris Dombrowski/Raleigh/IBM Rick Dayan/Raleigh/IBM Paul Benson/Raleigh/IBM Dave Challener/US/Lenovo/IDE Scott Dunham/Raleigh/IBM Ben Grimes/Raleigh/IBM Andy McNeill/Raleigh/IBM Howard Locker/US/Lenovo/IDE Jerry Pearce/US/Lenovo/IDE Joseph Lee/Raleigh/IBM David Rhoades/Raleigh/IBM Miriam M Davis/Raleigh/IBM Randy Springfield/Raleigh/IBM
Submitted date	09:02:47 AM EDT
* Owning division	PCD
Incentive program	(INC13) PC and xSeries Server
Lab	
* Technology code	
Patent value tool (PVT) score	

Inventors with a Blue Pages entry

Inventors: James Hoff/US/Lenovo/IDE@IBMUS, Jim Ward/Raleigh/IBM, Dave Challener/US/Lenovo/IDE@IBMUS, Howard Locker/US/Lenovo/IDE@ibmus

Inventor Name	Inventor Serial	Div/Dept	Inventor Phone	Manager Name
> Hoff, James	689283	44/C5AA	526-2980	Dion II, N.A. (Norman)
Ward, James P.	000718	44/C5AA	444-2410	Dion II, N.A. (Norman)
Challener, David C. (Dave)	048542	44/GG6A	443-6891	Clark, L. W. (Jeffrey)
Locker, Howard J.	459199	44/26GA	444-2540	Janick, Jan M.

> denotes primary contact

Inventors without a Blue Pages entry

Invention Development Team Information
Main Idea

RPS8-2001-0130 Secure Pin entry for TCPA - continued

To view the Main Idea of this disclosure, open the "Main Idea" document from the view
***Critical Questions (Questions 1-9 must be answered in English)**

***Question 1**
On what date was the invention workable? **Please format the date as MM/DD/YYYY**
(Workable means i.e. when you know that your design will solve the problem)

***Question 2** ○ Yes ● No
Is there any planned or actual publication or disclosure of your invention to anyone outside IBM?
If yes, Enter the name of each publication or patent and the date published below.
Publication/Patent:
Date Published or Issued:

Are you aware of any publications, products or patents that relate to this invention? ○ Yes ● No
If yes, Enter the name of each publication or patent and the date published below.
Publication/Patent:
Date Published or Issued:

***Question 3** ○ Yes ● No
Has the subject matter of the invention or a product incorporating the invention been sold, used internally in manufacturing, announced for sale, or included in a proposal?

Is a sale, use in manufacturing, product announcement, or proposal planned? ● Yes ○ No
If Yes, identify the product if known and indicate the date or planned date of sale, announcements, or proposal and to whom the sale, announcement or proposal has been or will be made.
Product:1q02 Desktop/Thinkpad
Version/Release:
Code Name:
Date:1q02
To Whom:
If more than one, use cut and paste and append as necessary in the field provided.

***Question 4** ○ Yes ● No
Was the subject matter of your invention or a product incorporating your invention used in public, e.g., outside IBM or in the presence of non-IBMers?
If yes, give a date. **Please format the date as MM/DD/YYYY**

***Question 5** ○ Yes ● No
Have you ever discussed your invention with others not employed at IBM?
If yes, identify individuals and date discussed. Fill in the text area with the following information, the names of the individuals, the employer, date discussed, under CDA, and CDA #.

***Question 6** ○ Yes ● No ○ Not sure
Was the invention, in any way, started or developed under a government contract or project?
If Yes, enter the contract number

RPS8-2001-0130 Secure Pin entry for TCPA - continued

***Question 7**
Was the invention made in the course of any alliance, joint development or other contract activities?
If **Yes**, enter the following:

○ Yes ● No ○ Not Sure

Name of Alliance, Contractor or Joint Developer

Contract ID number

Relationship contact name

Relationship contact E-mail

Relationship contact phone

***Question 8**
Have you, or any of the other inventors, submitted this same invention disclosure or similar invention disclosure previously?

○ Yes ● No

If Yes, please provide disclosure number below:

***Question 9**
Are you, or any of the other inventors, aware of any related inventions disclosures submitted by anyone in IBM previously?

○ Yes ● No

If Yes, please provide the docket or disclosure number or any other identifying information below:

Question 10
What type of companies do you expect to compete with inventions of this type? *Check all that apply.*

- ☐ Manufacturers of enterprise servers
- ☒ Manufacturers of entry servers
- ☒ Manufacturers of workstations
- ☒ Manufacturers of PC's
- ☐ Non-computer manufacturers
- ☒ Developers of operating systems
- ☒ Developers of networking software
- ☒ Developers of application software
- ☒ Integrated solution providers
- ☐ Service providers
- ☐ Other (Please specify below)

Question 11
If the invention relates to a product or service that is outside the scope of your business unit, please recommend IBM business unit(s), IBM location(s) or individual(s) within IBM that you think would provide a good evaluation of your invention:

***Patent Value Tool (Optional – this may be used by the inventor and attorney to assist with the evaluati...**
Evaluation
Search Information
Search Office Information
Final Decision
Post Disclosure Text & Drawings

Main Idea for Disclosure RPS8-2001-0130
Prepared for and/or by an IBM Attorney - IBM Confidential
Archived On 01:02:11 AM

Title of disclosure (in English)
Secure Pin entry for TCPA

Main Idea

1. Describe your invention, stating the problem solved (if appropriate), and indicating the advantages of using the invention.
IBM is a charter member of TCPA (Trusted Platform Security Alliance). The product of this consortium is a security chip in desktop systems that allows for secure cryptographic operations (such as digital signature) as well as system integrity measurements. These systems can guarantee that a digital signature originated in a particular platform, but they cannot as yet guarantee that it was done at the behest of a user sitting at the keyboard. Furthermore, a method is needed to protect against 'trojan horse' sniffer level attacks whereby the valid user authorization is recorded and then replayed at a later time.

This invention provides a secure path to the IBM TCPA chip so that pin entry is not sniffable by software.

2. How does the invention solve the problem or achieve an advantage,(a description of "the invention", including figures inline as appropriate)?
Basically we note that the chip is no longer soldered on the motherboard, but is now on a daughtercard, plugged into the motherboard. As such, with authorization, it is possible to unplug the card and put in an interposer between the card and the motherboard. This interposer would normally do nothing, but at such time as a PIN were required, instead of entering the pin through the keyboard where it would be transmitted to the daughter card over a sniffable bus, the pin would be enterred into a keypad that would directly enter the PIN into the daughter card.

This interposer/keypad is ideal for our business as it
1) adds no cost to the product
2) Can be charged for by those interested in hightened security
3) Solves the trusted path problem we are asked about by customers

Specifically, we teach the following implementation:
The interposer would intercept all keyboard input before it is routed to the superio (kbclk and kbdata signals). If the "trusted pin" switch is on (high), then the keyboard PIN data would be rerouted to the TPM, otherwise it is passed through to the superio. The Trusted Pin Switch would be implemented by a GPIO signal that is controllable by software. First generation TPMs are LPC devices. Therefore the interposer requires an LPC interface with the TPM to communicate the PIN data. This implies that the interposer can act as a bus master on the LPC bus.

1.) TSS sends a "Secure PIN Command" to the interposer . The secure pin command only contains the tag, ordinal, and any data non-authorization data.
2.) The interposer filters all keyboard input following successful receipt of Secure Pin Command.
3.) Interposer receives input from the keyboard and buffers the PIN data.
4.) Interposer initiates an Authorization Session with the TPM by sending TPM_OAIP command.
5.) TPM
-creates a session
-Creates a Handle H0

-Generates Nonce N0
-Saves N0 and H0

6.) TPM
-sends (N0,H0) on the wire to Interposer.

7.) Interposer
-Generates N1
-Computes Authorization = HMAC(PIN data, Ordinal, ...etc) ..as outlined by the TCPA spec for each command.

8.) Interposer
-sends HMAC(PIN data,Ordinal....etc) on the wire.

9.) TPM
-Retrieves N0 and Actual PIN data. (previously stored data)
-Computes HMAC(Actual PIN, Ordinal, ...)
-Verify computation with Authorization packet sent from Interposer.
-If they do no compare return TPM_E_InvalidAuth
-Execute Secure Pin Command and generate return code.
-Destroy the Session (This assumes that Authorization must be performed for EVERY Secure Pin Command.)
-Release the Secure PIN GPIO

We note that because the TPM uses the HMAC structure, this device need not be put as an interposer to the design, but could actually be placed anywhere that the computer has access to. The important thing is that this additional device
1) Be routable by software as a virtual interposer to the TPM
2) The entry of the pass phrase which generates the PIN data not be in a memory location sniffable by the rest of the system
3) The calculation of the HMAC be done internal to the device
4) The results be sent on their way to the TPM

3. If the same advantage or problem has been identified by others (inside/outside IBM), how have those others solved it and does your solution differ and why is it better?

4. If the invention is implemented in a product or prototype, include technical details, purpose, disclosure details to others and the date of that implementation.